

Gartner

Identity & Access Management Summit 2008

Deliver Security and Business Benefits
through Mature IAM Programs



23-24 JUNE 2008 ROYAL LANCASTER HOTEL, LONDON
europe.gartner.com/iam

KEYNOTE SPEAKER



Giles Hogben
IAM Expert
ENISA

SUMMIT CO-CHAIRS



Ant Allan
Research VP
Gartner



Ray Wagner
Managing VP
Gartner

REGISTER BY 25 APRIL 2008
AND SAVE €300

Gartner
Identity & Access
Management
Summit 2008



Better approaches, processes, and innovative technologies

Introduction from the Summit Chairs

Whoever your users are – your workforce, your business partners, your online customers – managing their digital identities and their access to your systems is critical – and this is the core focus of identity and access management (IAM).

While traditional information security programs have focused on managing risk by “keeping the bad guys out” through protective measures, such as next-generation firewalls, managing risk by focusing on “letting the good guys in” has become increasingly important, and identity and access management (IAM) is now established as a cornerstone of information security.

What’s more, recent IAM investment has also realized benefits in both regulatory compliance and IT governance. Thus, IAM makes a significant contribution to one of the six critical imperatives for your organization; namely, to manage risk, compliance and enterprise governance.

But realizing all the benefits from an IAM program is not trivial. Making the *business case*, engaging all stakeholders across the business, developing the *right processes*, selecting and implementing the *right technologies*, and orchestrating all the elements within a well-governed IAM program remain significant challenges.

Gartner’s **2nd Annual Identity & Access Management Summit** in EMEA addresses these challenges facing IAM programs and professionals tasked with making them work.

This year’s summit focuses on three main elements:

- a) **The *business and culture* issues.** You need to be able to articulate the business value of IAM, considering not just the return on investment, but also on risk management, regulatory and stakeholder exposure, and the reliability of business operations.
- b) **The *process* issue.** You must consider IAM as a *process*, and not purely as a set of technologies. While IAM projects frequently begin as technical solutions to tactical problems, that approach does not provide a good foundation for a complex program.
- c) **The *technology* issue.** While IAM is far more than just a set of technologies, no IAM program can succeed without understanding the *technologies* needed. Core technologies continue to be important, but we see new innovations that focus on particular drivers and benefits. It is crucial that you understand how to mix the old and the new.

Furthermore, this year’s program brings together a powerful concentration of Gartner IAM expertise, a keynote presentation from ENISA, and a series of case studies to give you the tools you need to deliver both the security and business benefits from your IAM initiatives.

We hope you can join us!



Ant Allan
Research VP, Gartner



Ray Wagner
Managing VP, Gartner

KEY TOPICS

Key elements of an IAM program

Alignment of business processes, requirements and systems

Future of IAM technologies

Strategies for executive support for IAM initiatives

Effective cost/benefit analyses for IAM project investment

IAM contribution to risk management, compliance and governance

Practical model for communicating IAM ROI

Modeling IAM architectures at an enterprise level

Enterprise privacy laws in IAM strategy

Federated identity management

New authentication methods in heterogeneous environments

Best practices for a successful role life-cycle management program

Rise of service-based identity management

Combining IAM functionality with NAC

IAM in a context-driven architecture

The NEW TRACKS for 2008

Following on from the success of last year's event and based on the survey results and continuous research, the **2nd Annual Identity & Access Management Summit** in EMEA is built along three main tracks:

1 **Planning, Building and Governing Successful IAM Programs**

An IAM program should not start with technology, but rather with an understanding of how your organization currently handles users' digital identities and the importance it places on these as a business asset. From this understanding flow the strategic plan, the architecture, the controls, and the processes. You also need to articulate the business value using the 4I model and establish roles for IAM governance.

2 **Implementing IAM Technologies for Efficiency and Effectiveness**

IAM has become a core IT infrastructure that touches every part of the enterprise. This track focuses on the key technologies that make significant contributions to administrative efficiencies and effective controls.

3 **Emerging Technologies for Innovative and Agile IAM Programs**

Your IAM program, like your organization, must remain innovative and agile. You can embrace new IAM technologies that allow you to meet pressing needs in a more timely way or facilitate IAM process optimization. You also need to consider how you can augment your IAM program with technologies not traditionally considered as IAM, such as security information and event management and network access control.

V **NEW VIRTUAL TRACK: Best Practices for IAM Projects – and Pitfalls to Avoid**

From over a decade of experience with IAM projects, the do's and don'ts are clear. This track focuses on those tasks and actions that optimize the efficiency or effectiveness of IAM itself – the standard benchmarks for world-class operations. And on the things that waste time and money – and which in the worst cases can completely derail projects.

WHO SHOULD ATTEND?

Senior IT and Business Professionals including:

- CISO, CSOs and their teams
- VPs, Directors and Managers of IT Security
- IAM Project Managers
- IT Security, Audit, Risk Managers and Specialist
- IT Quality & Compliance Managers
- IT Governance Managers
- Compliance Officers
- Enterprise and Solution Architects
- Technical Architects

With responsibilities encompassing Strategy Development, Strategic Architecture Development, Security Integration & Management, Services & Product Evaluation.

The event is relevant to all organizations including Financial Services, Telecoms, Manufacturing, Public Sector, Healthcare, Retail/Wholesale, Construction, Professional Services, Oil & Gas, Media, Healthcare and Pharmaceutical, Utilities, Transport & Logistics.

WHY ATTEND?

- By ensuring that people have the access they need when they need it, IAM makes its contribution to improving your workforce effectiveness.
- Effective web access management, identity federation and strong online customer security help organizations attract and retain customers.
- For a long time, organizations have seen benefits from automated workflow in identity administration through improved service levels and cost containment. Thus, IAM can help you to maximize performance, profitability and, hence, competitiveness.
- IAM processes aligned with business needs and facilitated by identity administration technologies improve critical identity-focused business processes and workflows.
- IAM can help you build an innovative and agile organization, too. By abstracting identity management and access controls from applications, IAM lets your application developers focus on business needs and lets them make innovative use of new technologies that contribute to your overall business agility.

For over 25 years, Gartner analysts have been the trusted advisors to many of the world's largest and most demanding organizations. No one sees the implications of technology so clearly, so consistently. Gartner analysts draw constantly from the real-life challenges and solutions experienced by more than 45,000 clients worldwide. The value of this resource, combined with our deep analysis of technology vendors, is unrivaled. The Gartner Identity & Access Management Summit brings a level of experience and expertise that you simply cannot get anywhere else.



Ant Allan
Research VP

"Again and again we see compliance and audit requirements forcing organizations to provide greater control over and accountability for the use of shared superuser accounts. But how?"

Focus Areas: User authentication; Shared-account password management; Superuser privilege management; Other IAM technologies; IAM program management



Carsten Casper
Research Director

"Violating privacy laws is more than crossing a red light. Protecting privacy is more than just buckling up. Manage privacy, not the law."

Focus Areas: Privacy legislation; EU and cross-border privacy; Privacy certifications; Compliance



Philip Dawson
Research VP

"Virtualization, Infrastructure and IAM – remember in this complex web the apps running on servers have identity too and virtualization only complicates the situation if not from only a licensing but also a management and availability perspective."

Focus Areas: Virtualization (server, infrastructure and process); Server selection (Workloads Server Platforms etc); ERP infrastructure selection



Avivah Litan
VP Distinguished Analyst

"New trends in criminal techniques make it especially difficult to detect fraudsters, whether they are opening new accounts, registering for new services or shopping for digital goods."

Focus Areas: Identity theft related fraud; Online banking and credit card fraud detection systems; Transaction anomaly (fraud) detection systems; Anti-phishing solutions; Consumer authentication applications; Identity networks; B2C web-payment software and payment gateways; Back-end credit card/EFT (ACH) processing/networks; B2C electronic bill



Jeff Mann
Research VP

"Customers often tell me that IAM policies get in the way of what they need to do. A context-driven architecture can wrap up IAM and other services to make all applications more usable."

Focus Areas: Context-driven architectures (CoDA); Collaboration; High performance workplace



Mark Nicolett
VP Distinguished Analyst

"Many organizations are initiating user activity monitoring projects in order to discover inappropriate data access and to become compliant with requirements such as PCI."

Focus Areas: Security information and event management (SIEM); Patch management; Vulnerability Management; Network access control



Eric Ouellet
Research VP

"CMF/DLP tools provide value well beyond simply logging or blocking of undesirable events. Resource and accessibility audits are natural fit for leveraging these capabilities."

Focus Areas: Content monitoring and filtering and data loss prevention (CMF/DLP); Resource and access audits; PKI/PKO integration; Other IAM



Earl Perkins
Research VP

"A point has been reached in identity and access management market maturity where one can start to distinguish between strategic plays and operational conveniences."

Focus Areas: Identity management products and services; IAM processes; Identity and privacy issues; Oracle and SAP security and identity frameworks; Web services, SOA and SaaS security and identity issues; Secure software development lifecycle; Virtualization infrastructures



Tom Scholtz
Research VP

"Don't expect your business to continue funding big ticket IAM projects if you can't communicate the value of IAM in business terms."

Focus Areas: Security strategy; Security architecture; Security organization; Investment justification; Secure outsourcing; BCP/DRP

Keynote Speakers

Giles Hogben IAM Expert, ENISA



Giles Hogben is an expert on identity management and authentication technologies working at ENISA, the European Network and Information Security Agency in Greece. He has published numerous papers on identity management, privacy and the semantic Web, including a widely cited report on "Security Issues and Recommendations for Online Social Networks". Before joining ENISA, Giles was a researcher at the Joint Research Centre in Ispra, and led work on private credentials in the EU PRIME project (Privacy and Identity Management for Europe). He graduated from Oxford University in 1994.

Ant Allan Research VP, Gartner



Ant Allan, Ph.D., is a research vice president in Gartner Research. He is a core member of the identity and access management (IAM) research community and specializes in IAM program management, user authentication, shared-account password management and superuser privilege management. Prior to joining Gartner, Ant worked for two years as a product manager for security software products with a U.K. distributor. Before that, he worked for seven years in information security management for GA Life, focusing on IBM OS/390 RACF and information security policy, after short stints in application development and information technology training.



Gregg Kreizman Research Director

"The pressure to improve user convenience continues to trump operational efficiency improvements as the primary consideration for single sign-on initiatives."

Focus Areas: Enterprise single sign-on (ESSO); Electronic signature; Security architecture; Federation and personal identity frameworks (PIFs); Other IAM



Lawrence Orans Research Director

"Enterprises need to take the anonymity out of networking. Integrating network access control with identity and access management will help organizations better protect their intellectual property and sensitive internal data."

Focus Areas: SIP security; VOIP security; IM security; Proxy servers; Web/URL filtering; Scan and block; Network access control (NAC)



Ray Wagner Managing VP

"It's time to join the IAM mainstream, where technology, process, and architecture come together."

Focus Areas: Web access management; Identity federation; Rights management

End-User Case Study Speakers

To complement Gartner research, advice and direction, the Identity & Access Management Summit features end-user case studies from across Europe, covering different industries and topics. These case studies will address pragmatic and real-life experiences of the end-user community, to provide you with insight into lessons learned and pitfalls to avoid.

Keep updated with further developments at europe.gartner.com/iam



Sylvère Léger
Chief Security Officer,
AGF Group France

Implementing Role-Based Access Control (RBAC) and Segregation of Duties (SOD)

AGF, the French subsidiary of Allianz Group, wishes to continue its Identity Management project with RBAC and SOD approaches. But the gap between theory and reality could be important. Which approaches could be explored to integrate compliance and business requirements?

- What is the real significance of RBAC and SOD for a company?
- How can we conceive Business Roles and implement them in IT systems for increased efficiency and response?
- How can we enforce a SOD matrix compatible with real risks and budget constraint?



Ingrid Melve
Chief Technology
Officer,
UNINETT

Challenges and Solutions of Scaling Identity Management and Federated Access

The Norwegian Ministry of Education and Research recognized the need for a common IAM solution in the educational community as one of the prerequisites for attaining its ICT vision. The FEIDE project enables distributed identity management and federated access.

- What are the best practices for agreeing on standards for local identity and shared access management?
- What are the benefits of such an approach?
- What are the main elements of success?



Andre Steffens, Group
IT Architect,
Metropolitan Holdings

The 10 Do's and Don'ts of IAM Projects – Mistakes to Avoid

Metropolitan embarked on an IAM initiative two and half years ago. During this time, they faced many challenges, primarily in business buy-in and lack of common vision in the IT department. This session focuses on the metropolitan roadmap for launching an IAM initiative.

- How do you ensure that you have business buy-in for your IAM initiative?
- What skills do you need to have to drive the project?
- What compromises you may need to make to get the project started?

Panel Discussion Identity Assurance: Establishing Common Levels of Trust

Federations inside the enterprise have been advancing globally, but growth outside the enterprise has struggled, requiring better definition of trust, business rules for governing that trust, and some means of certifying or accrediting levels of trust offered by organizations and federations. This panel will include several end deployers sharing individual case studies and experiences, discussing the Identity Assurance Framework, a program under development within the Liberty Alliance to define such a Framework, and discuss the levels of assurance and resulting certification and accreditation program that will advance this concept into global commercial acceptance.

- Vijay Takanti**, TSCP
Jan Riis, Digital Health Denmark
Robert Temple, BT

AGENDA AT A GLANCE

Experience a unique mix of Gartner analyst presentations, guest keynotes, real-life case studies, interactive panels and selected solution provider sessions adding up to a cutting edge program agenda.

SUNDAY 22 JUNE

18:00 – 19:30 Registration and Information

MONDAY 23 JUNE

07:30 Registration and Information

08:30 – 08:45 Conference Opening

08:45 – 11:15 Plenary Sessions

11:45 – 13:15 Track Breakout Sessions

13:15 – 14:15 Lunch & Solution Showcase

14:15 – 18:00 Track Breakout Sessions

18:00 – 20:00 Networking Drinks Reception

TUESDAY 24 JUNE

08:30 – 12:00 Track Breakout Sessions

12:00 – 13:00 Lunch & Solution Showcase

13:00 – 13:50 Plenary Session

14:00 – 16:00 Track Breakout Sessions

16:15 – 17:00 Plenary Session

17:00 Conference Close

PLENARY SESSIONS

Taking Care of Business: How IAM Contributes to Your Key Business Imperatives

IAM is now established as a cornerstone of information security. Recent IAM investment has realized benefits in both regulatory compliance and IT governance. Thus, IAM makes a significant contribution to one of your six critical business imperatives. But an IAM program can deliver more than this!

- What are the key elements of an IAM program?
- How does IAM contribute towards risk management, compliance and enterprise governance?
- How does IAM contribute towards other critical business imperatives?

Ant Allan, Gartner

Digital Cocktail Party: Social Media Meets IAM

You may not have noticed, but online social networks have all the characteristics of a full-blown IAM system. They collect and organize huge amounts of personal data, they restrict access to that data based on credentials such as membership of a group, and they provide user-interfaces for defining access rules. Social media have crept up on us from behind, but they are fast becoming an important part of the IAM landscape.

- What benefits does social networking offer to IAM?
- What dangers do enterprises need to be aware of and what policies can help to protect them?
- How are social media evolving and what implications does this have for IAM?

Giles Hogben, IAM Expert, ENISA

Best Practices for Vendor Selection: The Gartner IAM Magic Quadrants

This presentation will introduce and discuss the Gartner Magic Quadrants that cover three key identity and access management technologies: Enterprise Single Sign-On, User Provisioning and Web Access Management.

- What trends and product differentiators contribute to Magic Quadrant positioning in each technology?
- What is the future of the technologies represented?
- Do single-vendor suites provide the best approach to an enterprise IAM solution?

Gregg Kreizman, Earl Perkins and Ray Wagner, Gartner

Does Cutting Costs Spell the Death of Your Pet IAM Project

The CIO of XYZ Bank is looking to cut costs by axing one of three projects within the bank's IAM program. The sponsoring manager of each project will make the case for his project. In this lively role-play session, you can help the CIO decide!

- Would cutting it leave the company exposed to risk?
- Does it deliver value against one of the critical imperatives?
- Can the bank actually achieve cost cutting through the project?

Ray Wagner, Gartner



An IAM program should not start with technology, but rather with an understanding of how your organization currently handles users' digital identities and the importance it places on these as a business asset. From this understanding flow the strategic plan, the architecture, the controls, and the processes. You also need to articulate the business value using the 4I model and establish roles for IAM governance.

Articulating the Business Value of IAM

The IAM program is a big ticket budget item. As budgets begin to tighten it will become increasingly difficult to justify IAM expenditures. This presentation will share:

- Strategies for obtaining and maintaining executive support for IAM initiatives
- A practical model for communicating the business value of an IAM program
- Techniques for effective cost/benefit analyses for IAM project investment

Tom Scholtz

Best Practices for IAM Program Governance and Project Management

IAM programs can be complex and take years to establish. While IAM can contribute towards IT and enterprise governance, this requires a higher level of governance across all IAM. Governance addresses the efficient and effective use of IAM, and that demands effective IAM project management as well.

- How do IAM technologies contribute to IAM governance?
- What are best practices IAM governance?
- How can we use the systems development life cycle (SDLC) for an IAM project?

Ray Wagner

Know Your IAM Processes to Get the Most Out of Your IAM Programs

Processes are foundational to IAM. While technologies provide automation and efficiency, those that overlay broken or disjointed processes won't achieve the desired results. Enterprises must understand their core IAM processes to move towards a desired future state.

- What are the core IAM processes and how do they relate to other security and business processes?
- How can you use IAM processes to improve operational efficiency?
- How can you measure process improvements and demonstrate process maturity?

Gregg Kreizman

Best Practices for Building an IAM Architecture

Designing an IAM infrastructure is a complex architectural challenge. Doing it in isolation from other security and enterprise architecture initiatives is a recipe for disaster. Key issues to be addressed in this session:

- What are the most effective contents and structures for security architecture, and how do these fit with EA?
- How should enterprises model IAM architectures?
- What are IAM architecture best practices?

Gregg Kreizman and Tom Scholtz

Identity Management and Privacy Legislation: Love or Hate?

IAM is affected by privacy legislation in many ways. This presentation will examine win-win situations and potential conflicts regarding legal requirements, technical reality and economic rationale by looking at the following key issues:

- IAM workflow needs to involve notification steps, including those in cross-border data transfer scenarios
- Identity storage needs to consider separation for different jurisdictions, and internationally different approaches of law enforcement
- An IAM strategy should consider the enterprise's privacy profile

Carsten Casper

TAILOR YOUR OWN AGENDA IN ADVANCE!

To enable you to build your own personal agenda and select the sessions that are relevant to you, please use our **online Agenda Builder** to ensure you make the right decisions and get the best value from the Summit.

For details please visit
www.europe.gartner.com/iam

IAM has become a core IT infrastructure that touches every part of the enterprise. This track focuses on the key technologies that make significant contributions to administrative efficiencies and effective controls.

Federation Best Practices at the Dawn of the Emerging Personal Identity Framework

Identity federation technology is ready to deploy and there are many successful implementations. Personal identity frameworks are evolving to build on federation's success and to improve user convenience and privacy protections.

- What are the best practices for identity federations?
- How are personal identity frameworks (PIFs) leveraging and improving upon federations?
- What are the future directions for federation technologies and PIFs?

Gregg Kreizman and **Ray Wagner**

SIEM for Identity and Access Monitoring

Security information and event management (SIEM) technology provides the ability to broadly monitor both privileged and application user activity. We provide advice on how to use SIEM to complement IAM audit, and how to integrate SIEM and IAM to achieve exception monitoring.

- What are the capabilities and limitations of IAM audit functions?
- How can SIEM technology be used to fill IAM audit gaps?
- How should organizations select SIEM vendors and deploy SIEM technology?

Mark Nicolett

Best Practices for Selecting and Implementing New Authentication Methods

Enterprises are increasingly seeking to replace or supplement passwords with new, stronger authentication methods. But the choice of authentication methods is wider than ever – and different methods are likely appropriate to different use cases.

- What is the range of authentication methods available and in use today?
- How can enterprises select the methods that best fit different use cases?
- What is the most effective way to implement new authentication methods in heterogeneous environments?

Ant Allan

The Access Control Dilemma: Managing Authorization for Applications and Services

Historically, we have provided application access infrastructure, where applications are able to recognize which user can use specific capabilities and resources. To date, most management resides in applications, resulting in a kaleidoscope of authorization management systems. Can it be abstracted to the infrastructure?

- What is the current state of authorization management today?
- What are the pain points that lead customers to consider an authorization management solution?
- What options are available for solving authorization management issues?

Earl Perkins

Will the Real User Please Stand Up?

We position best practices for identifying and verifying online consumers and transaction against a background of increasing attacks against sensitive personal and financial data. We also examine and recommend methods for authenticating sites to users.

- What are the latest trends in attacks, and how are enterprises and customers responding?
- What are best practices in authentication, transaction verification and fraud detection?
- What methods are available for authenticating e-commerce sites and fostering user confidence?

Avivah Litan

The Secret to Good IAM Deployments: Best Practices for Role Management

Effective enterprise role management is possible. Organizations have enhanced their role framework and tied business and IT roles together in order to present a single face to the enterprise.

- What does role lifecycle management mean in today's identity and access management solutions?
- How have role lifecycle management processes and technologies changed in the last year?
- What are the best practices for implementing and maintaining a successful role life cycle management program?

Earl Perkins

Your IAM program, like your organization, must remain innovative and agile. You can embrace new IAM technologies that allow you to meet pressing needs in a more timely way or facilitate IAM process optimization. You also need to consider how you can augment your IAM program with technologies not traditionally considered as IAM, such as security information and event management and network access control.

CMF/DLP and Data Discovery: How It Will Impact Your IAM Environments

Many organizations have introduced new CMF/DLP capabilities within their environments to better control and protect sensitive assets at the perimeter and end points. As these tools become refocused and redirected to support broad based data discovery initiatives they will impact the traditional view of IAM audits.

- How are CMF/DLP technologies being used for data discovery?
- What is the impact of CMF/DLP tools to IAM?
- How can organizations better integrate CMF/DLP in IAM audits?

Eric Ouellet

Virtualization and IAM

Virtualization projects are emerging all over the portfolio. This session looks at how to leverage and unify infrastructure virtualization efforts and the impact of virtualization from an IAM perspective.

- What is the impact of virtualization on the portfolio?
- How will IAM planning have to evolve to adequately take into account the capabilities offered by virtualization?
- What is the impact of IAM for the applications, VMs and management tools in virtualized infrastructure?

Philip Dawson

Identity at Your Service(s): The Rise of Service-Based Identity Management

Will there ever be a day when customers can “buy” managed IAM services, rather than installing products within their enterprise? Is that day already here? Do IAM products embrace service based architectures to make implementations easier, whether in-house or by service providers?

- What is the current state of managed IAM services and service-based IAM architecture?
- How viable is true service-based IAM? What form will it take?
- What are the key questions customers must ask before using managed IAM services or service-based IAM?

Earl Perkins

Identity Aware Networks: Where IAM Meets Network Access Control (NAC)

Who are you and what are you doing on my network? Concerns over regulatory compliance and insider threats have brought this question to the forefront. Combining IAM functionality with NAC is the key to answering it.

- What are the benefits of integrating NAC and IAM?
- Which vendors are leading the way in integrating NAC and IAM?
- What are the best practices for building identity aware networks?

Lawrence Orans

Getting to the Problem of the Root: Best Practices for Managing Superuser Privileges and Shared Account Passwords

Organizations are under increasing pressure to reduce the number of users having permanent full superuser privileges, and to implement better control over, and greater accountability for, use of shared accounts with like privileges.

- How can you most efficiently and effectively contain use of full superuser privileges?
- How can you manage individuals' use of shared privileged accounts in a controlled and auditable manner?
- What are the best practices for dealing with embedded application-to-application passwords?

Ant Allan

What You Need Is What You Get: IAM in a Context-Driven Architecture

The imminent arrival of what you need is what you get (WYNIWYG) services will demand that organizations adopt Context Driven Architecture (CoDA). New IAM services will be required to give end users what they need in 2012.

- How will major shifts in communication technologies create this new class of context aware services?
- What new models will be required to deliver these services?
- How can security architects prepare to support CoDA?

Jeff Mann

From over a decade of experience with IAM projects, the do's and don'ts are clear. This track focuses on those tasks and actions that optimize the efficiency or effectiveness of IAM itself – the standard benchmarks for world-class operations. And on the things that waste time and money –and which in the worst cases can completely derail projects.

Federation Best Practices at the Dawn of the Emerging Personal Identity Framework

Identity federation technology is ready to deploy and there are many successful implementations. Personal identity frameworks are evolving to build on federation's success and to improve user convenience and privacy protections.

- What are the best practices for identity federations?
- How are personal identity frameworks (PIFs) leveraging and improving upon federations?
- What are the future directions for federation technologies and PIFs?

Gregg Kreizman and Ray Wagner

Best Practices for IAM Program Governance and Project Management

IAM programs can be complex and take years to establish. While IAM can contribute towards IT and enterprise governance, this requires a higher level of governance across all IAM. Governance addresses the efficient and effective use of IAM, and that demands effective IAM project management as well.

- How do IAM technologies contribute to IAM governance?
- What are best practices IAM governance?
- How can we use the systems development life cycle (SDLC) for an IAM project?

Ray Wagner

Best Practices for Selecting and Implementing New Authentication Methods

Enterprises are increasingly seeking to replace or supplement passwords with new, stronger authentication methods. But the choice of authentication methods is wider than ever – and different methods are likely appropriate to different use cases.

- What is the range of authentication methods available and in use today?
- How can enterprises select the methods that best fit different use cases?
- What is the most effective way to implement new authentication methods in heterogeneous environments?

Ant Allan

Best Practices for Building an IAM Architecture

Designing an IAM infrastructure is a complex architectural challenge. Doing it in isolation from other security and enterprise architecture initiatives is a recipe for disaster. Key issues to be addressed in this session:

- What are the most effective contents and structures for security architecture, and how do these fit with EA?
- How should enterprises model IAM architectures?
- What are IAM architecture best practices?

Gregg Kreizman and Tom Scholtz

Getting to the Problem of the Root: Best Practices for Managing Superuser Privileges and Shared Account Passwords

Organizations are under increasing pressure to reduce the number of users having permanent full superuser privileges, and to implement better control over, and greater accountability for, use of shared accounts with like privileges.

- How can you most efficiently and effectively contain use of full superuser privileges?
- How can you manage individuals' use of shared privileged accounts in a controlled and auditable manner?
- What are the best practices for dealing with embedded application-to-application passwords?

Ant Allan

The Secret to Good IAM Deployments: Best Practices for Role Management

Effective enterprise role management is possible. Organizations have enhanced their role framework and tied business and IT roles together in order to present a single face to the enterprise.

- What does role lifecycle management mean in today's identity and access management solutions?
- How have role lifecycle management processes and technologies changed in the last year?
- What are the best practices for implementing and maintaining a successful role life cycle management program?

Earl Perkins

Your own personalized solution provider shortlist

To maximize the event's relevance to you, we'll help you develop a shortlist of technology providers that can meet your own unique needs. This includes exclusive access to some of the world's leading technology providers in a variety of settings. Design your own program by combining the Solution Showcase, sponsor presentations and the networking drinks receptions for informal relationship building.

SPONSORSHIP OPPORTUNITIES

For details please contact Darren McCormack or Nigel Murphy

Tel: +44 (0)1784 26 8387

Email: Darren.mccormack@gartner.com

Tel: +44 (0)1784 26 7055

Email: Nigel.murphy@gartner.com

PLATINUM SPONSORS



Evidian

Evidian is a European leader and one of the main vendors worldwide in IAM software. Evidian provides E-SSO, user provisioning, identity federation and access control for SOA and classical architectures, within a modular and integrated IAM suite. Evidian software helps organizations increase their agility, comply with regulations and reduce costs.

www.evidian.com



IBM

IBM is the world's largest information technology company, with 80 years of leadership in helping businesses innovate. IBM enables companies to maximize value and manage risks by effectively mapping their business strategy to their IT investment strategy. IBM offers a wide range of solutions and technologies to assist customers in planning, designing and implementing security solutions.

www.ibm.co.uk



VeriSign

VeriSign provides Internet Infrastructure Services for the digital world. We protect businesses and consumers online with our SSL certificates, authentication solutions and fraud detection services and we run the .com and .net registries. Operating in 75 countries, we serve over 400,000 customers and support over 30 billion interactions every day.

www.verisign.com



Media Partners

EXECUTIVE.IT

FINANCE ON WINDOWS



InformationAge

prime

Retailspeak



SECURE.IT

silicon.com



SILVER SPONSORS



Authentify

Authentify offers real-time, out-of-band authentication by synchronizing a web session with an automated telephone call to verify the actual individual behind a digital identity.

www.authentify.com



Aveksa

Aveksa provides the only enterprise access governance solution that automates certification of entitlements; enables role lifecycle management; and delivers unmatched visibility into user access rights.

www.aveksa.com



Courion

Courion is the Enterprise Provisioning and Access Compliance Expert for results-driven organizations. Courion's software solutions streamline operations and automate business processes.

www.courion.com



dns

dns is the leading provider of identity management professional services, offering services such as requirements definition, strategy formulation, expert implementation and ongoing operational management.

www.dns.co.uk



Giesecke & Devrient
Creating Confidence.

Giesecke & Devrient

Giesecke & Devrient is a leading provider of USB tokens, next generation mobility tokens and smart cards for telecommunications, electronic payments, transportation and IT security.

www.gi-de.com



Guardium

Guardium's database activity monitoring solution provides granular access controls for sensitive data, monitors all transactions including privileged user activities in real-time, and automates compliance controls.

www.guardium.com



Imprivata

Imprivata safeguards enterprise information assets by enabling secure and compliant employee access to networks and applications. Please visit us at

www.imprivata.com



Omada

Omada is a leading Microsoft Solution Provider for Advanced Role Based Access Control & Compliance in Identity Management.

www.omada.net



Ping Identity

Ping Identity provides secure Internet single sign-on software to over 150 customers. PingFederate®, rapidly deployable identity federation software, provides direct access to Internet applications.

www.pingidentity.com



Swivel Secure

Swivel's PINsafe enables tokenless two-factor authentication, via a one-time code from a mobile phone or browser. Now PINsafe M2F can authenticate Windows.

www.swivelsecure.com



TrustAlert

TrustAlert enables enterprises to increase the security of online critical systems, reducing administrative cost and improving user satisfaction by using easy to deploy certificate technology.

www.trustalert.com



Völcker Informatik AG

Völcker Informatik AG is one of the leading vendors for integrated Identity Management, User Provisioning and IT Compliance solutions.

www.voelcker.com

Gartner is the leading provider of research and analysis on the global information technology industry. Our goal is to support organizations as they drive innovation and growth through the use of technology.

As in our research, our events help clients make informed technology and business decisions by providing in-depth analysis and actionable advice on virtually all aspects of technology.

Gartner EMEA Events in 2008

Enterprise Networking & Communications Summit

23-24 April, London

Wireless & Mobile Summit

23-24 April, London

Business Process Management Summit

28-30 April, London

Symposium/ITxpo

11-14 May, Barcelona

Outsourcing & IT Services Summit

2-4 June, London

Enterprise Architecture Foundations Seminar

16-17 June, London

Identity & Access Management Summit

23-24 June, London

SOA & Application Development and Integration Summit

25-26 June, London

Symposium/ITxpo

18-20 August, Cape Town

Portals, Content & Collaboration Summit

10-11 September, London

Enterprise Architecture Summit

23-24 September, London

IT Security Summit

29 September-
1 October, London

Data Center Summit

21-23 October, Amsterdam

Symposium/ITxpo

3-7 November, Cannes

Enterprise Architecture Foundation Seminar

3-4 December, Amsterdam

Gartner Strategie & Technologie Konferenz

2-3 December, Frankfurt

Gartner US Events in 2008

Gartner IT Security Summit

2-4 June, Washington, D.C., USA

Identity & Access Management Summit

10-12 November, Florida, USA





How to Register

Online: europe.gartner.com/iam

Tel: +44 (0)20 8879 2430

Email: emea.registration@gartner.com

REGISTRATION RATES

Standard Rate: €2,195 + 17.5% VAT

Early Bird Rate: €1,895 + 17.5% VAT

(offer ends 25 April 2008)

Why register early?

- Save €300 on the standard conference rate
- Priority One-on-One booking with the analyst of your choice

Group discounts

4 for the price of 3!

Register as a team of 3 or more and:

- Receive one additional free pass
- Get preferential access, as a team, to your preferred analyst of choice
- Exclusive meeting rooms for intra-team meetings onsite, subject to availability

Note: available on the Standard Rate only one discount applies

Gartner Clients:

We also accept Gartner conference tickets as full payment. If you are a client with queries about tickets, please contact your sales representative or email emea.events@gartner.com

UPDATE YOUR PROFILE

Gartner Events realises that your time is precious. That's why we only want to send you information that is relevant to your role. Update your profile with us and we will only send you information that meets your needs. Visit experiencegartner.com

© Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a trademark of Gartner, Inc. or its affiliates. All other brands are trademarks of their respective owners. E&OE. IAMDM2100308



